REMARKS

Claims 2-22 are pending, of which claims 2 and 8 are independent method claims with corresponding independent computer program product claims 12 and 18. As indicated above, new dependent claim 22 has been added by this paper.

The Office Action rejected each of the pending independent claims (2, 8, 12, and 18) under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,434,918 to Kung et al. ("*Kung*") in view of U.S. Patent No. 5,838,790 to McAuliffe et al. ("*McAuliffe*"). Each of the pending dependent claims was rejected under 35 U.S.C. § 103(a) as being unpatentable over *Kung* in view of *McAuliffe* or over *Kung* in view of *McAuliffe* and U.S. Patent No. 6,161,185 to Guthrie et al. ("*Guthrie*").[1]

Applicants invention, as claimed for example in independent claim 2, relates to a method of verifying that a server is authorized to provide resources to a client. In accordance with the method, a client generates a server authentication request and transmits the request to the server. The method includes receiving an encrypted server authentication response from the server and decrypting the response. Unless the server authentication response indicates that the server is authorized to provide at least one resource to the client, the method disables one or more client functions.

Applicants' invention, as claimed for example in independent claim 8, also relates to a method of verifying that a server is authorized to provide resources to a client. Similar to claim 2, a client generates a server authentication request and transmits the request to the server. After an allotted period of time, the client determines that no response to the server authentication request has been received, interprets no response as an indication that the server is not authorized to provide resources to the client, and disables one or more client functions.

Kung discloses mutual authentication of a user and a server on a network without exchanging a user's password in clear text. Col. 2, ll. 16-19. The client transmits a logon ID to the server. Col. 1, ll. 53-54. The server retrieves a user password corresponding to the logon ID and uses the password to encrypt a random number. Col. 1, ll. 54-60. To decrypt the random number and authenticate the server, the user enters the password at the client. Col. 1, ll. 60-65.

[1]Applicants reserve the right to challenge *Kung, McAuliffe,* and *Guthrie* as a proper prior art references in the future. Accordingly, any statement in this response with respect to *Kung, McAuliffe,* and *Guthrie* is made merely assuming *arguendo* that *Kung, McAuliffe,* and *Guthrie* represent prior art and should not be interpreted as acquiescing the references asserted prior art status or teachings.

This random number is used as the encryption and decryption key for communication between the client and server. Col. 1, ll. 66-67. The client sends a message encrypted with the random number to the server to authenticate the user. Col. 1, l. 67 – col. 2, l. 4.

McAuliffe discloses an advertisement system. In particular, *McAuliffe* uses a key-dependent one-way hash function to generate fingerprints of both advertisements downloaded to a user's computer and an advertisement statistics file (storing statistics as to which advertisements are shown to users, for how long, and at what times) which is periodically uploaded to a remote central computer. Col. 3, ll. 42-49. The fingerprints allow for detection of any tampering with, modification of, or replacement of the advertisements and statistics file. Abstract; col. 3, ll. 49-58. Remedial action, such as disabling client software, is taken only after multiple incidents of tampering are detected within a short time period for the same user. Col. 11, ll. 4-17.

In order to establish a *prima facie* case of obviousness, "the prior art reference (or references when combined) must teach or suggest all the claim limitations." MPEP § 2143 (emphasis added). During examination, the pending claims are given their broadest reasonable interpretation, i.e., they are interpreted as broadly as their terms reasonably allow, consistent with the specification. MPEP §§ 2111 & 2111.01. The Office Action asserts that *Kung's* logon ID corresponds to Applicants' authentication request and that *Kung's* password encrypted random number corresponds to Applicants' authentication response. Office Action, pp. 3-4 (rejection of claims 2, 5, 8, 12, 15, 18 and 20). The Office Action concedes, however, that *Kung* fails to disclose disabling client functions, but asserts that *McAuliffe* teaches disabling client software after multiple incidents of tampering and that it would have been obvious to one of ordinary skill in the art to modify *Kung* to disable client functions when tampering is detected as taught in *McAuliffe*. *Id.*

To support its reasoning, the Office Action characterizes both *McAuliffe's* tampering detection, and Applicants' disabling one or more client functions when a server authentication response fails to indicate that the server is authorized to provide at least one resource to the client, as a "negative result of authentication." *Id.* Then, in justifying the combination of *Kung* and *McAuliffe*, the Office Action asserts that "[o]ne of ordinary skill would have been motivated to disable client functions in case of a negative result of authentication as taught in *McAuliffe* for making sure that the advertisements are properly displayed at a remote computer." *Id.* For the

reasons stated below, Applicants respectfully disagree with the Office Action's assertions, logic, and conclusions.

First, it is improper and unreasonable for the Office Action to interpret both *McAuliffe's* tampering detection and Applicants' disabling one or more client functions when a server authentication response fails to indicate that the server is authorized to provide at least one resource to the client, as simply and broadly as a "negative result of authentication." As discussed above, *McAuliffe* discloses authenticating that advertisements and statistics files have not been tampered with, modified or replaced. In contrast, Applicants' claim 2 recites "disabling one or more client functions unless the server authentication response indicates that the server is authorized to provide at least one resource to the client," and Applicants 'claim 8 recites "interpreting no response [to a server authentication request] as an indication that the server is not authorized to provide resources to the client" and "disabling one or more client functions." Merely applying a common label to both *McAuliffe's* tampering detection and Applicants' limitations does not make *McAuliffe's* tampering detection and Applicants' limitations the same for purposes of evaluating patentability. It is simply unreasonable to interpret Applicants' "disabling one or more client functions unless the server authentication response indicates that the server is authorized to provide at least one resource to the client," as found in claim 2, and "interpreting no response [to a server authentication request] as an indication that the server is not authorized to provide resources to the client" and "disabling one or more client functions," as found in claim 8, so broadly that *McAuliffe's* tampering detection represents the same limitation. Accordingly, even assuming *arguendo* that the combination of *Kung* and *McAuliffe* is proper, *Kung* and *McAuliffe* fail to teach or suggest all of the limitations of independent claims 2, 8, 12, and 18.

Second, the Office Action mixes the notions of authentication (confirming identity) and authorization (permission). "For a variety of reasons, suppliers or manufacturers of certain client systems may desire to allow only selected servers to provide network resources to their client systems." Specification, p. 3, ll. 15-17. However, as Applicants disclose, a client system and the operator of an unauthorized server could collude to override a conventional security system. *See* Specification, p. 4, ll. 5-12. That the client reaches the server that it intended to reach (confirmed identity), as disclosed in *Kung*, does not mean that the server is authorized (has permission) to provide resources to the client. The Office Action discusses the prior art only in terms of

authentication—not authorization, and therefore fails to establish a *prima facie* case of obviousness because, as indicated above, Applicants' independent claims recite "disabling one or more client functions unless the server authentication response indicates that the server is authorized to provide at least one resource to the client" (*see* claims 2 and 12), and "interpreting no response [to a server authentication request] as an indication that the server is not authorized to provide resources to the client" and "disabling one or more client functions" (see claims 8 and 18).

Not only must "the prior art reference (or references when combined) . . . teach or suggest all the claim limitations" to establish a *prima facie* case of obviousness, but also "[t]he teaching or suggestion to make the claimed combination . . . must . . . be found in the prior art, not in applicant's disclosure." MPEP § 2143. As discussed above, to justify the combination of *Kung* and *McAuliffe*, the Office Action asserts that "[o]ne of ordinary skill would have been motivated to disable client functions in case of a negative result of authentication as taught in *McAuliffe* for making sure that the advertisements are properly displayed at a remote computer." Office Action, p. 4 (rejection of claims 2, 5, 8, 12, 15, 18 and 20). Making sure that the advertisements are properly displayed at a remote computer is the motivation for practicing *McAuliffe*, which detects whether advertisements or a statistics file has been tampered with, modified, or replaced—the Office Action fails to note what role if any *Kung* may have to offer in this respect, and thus why one of ordinary skill in the art would be motivated to combine *Kung* and *McAuliffe*. To the contrary, *McAuliffe* discloses that the advertisements are stored locally and output when the remote computer is off-line, making *Kung's* authentication irrelevant at the time advertisements are displayed. *See, e.g.,* Abstract; col. 1. l. 66 – col. 2, l. 1; col. 3, ll. 22-38; col. 5, ll. 33-39. Accordingly, the Office Action's motivation appears to be taken from Applicants' disclosure and based on improper hindsight reasoning. MPEP § 2145(X)(A). Applicants respectfully submit, therefore, that by neglecting to provide a motivation from the prior art to combine *Kung* and *McAuliffe*, the Office Action has failed to establish a *prima facie* case of obviousness with respect to the pending claims.

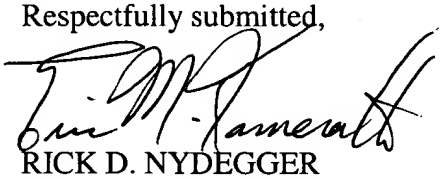
Dependent claims 7 and 17 recite that the server authentication request comprises an encryption key and a random number, and recite an act of encrypting the server authentication request. In contrast, the Office Action asserts with respect to dependent claims 7 and 17 that *Kung* teaches that a random number is created and encrypted by a symmetric encryption

algorithm on the server, as opposed to the client, using a retrieved user password in order to provide an encrypted password. Office Action, p. 4 (rejection of claims 7 and 17). Furthermore, as noted above, the Office Action asserts that *Kung's* logon ID corresponds to Applicants' authentication request, whereas *Kung's* password encrypted random number corresponds to Applicants' authentication response. Office Action, pp. 3-4 (rejection of claims 2, 5, 8, 12, 15, 18 and 20). Accordingly, Applicants respectfully submit that the rejection of claims 7 and 17 is improper and should be withdrawn because, at best, the Office Action merely asserts encryption of Applicants' server authentication response—not Applicants' server authentication request as claimed. Assuming *arguendo* that *Kung's* logon ID corresponds to Applicants' authentication request, at a minimum the Office Action should assert that *Kung* encrypts the logon ID in making a rejection of claims 7 and 17. Among other things, therefore, the combination of *Kung* and *McAuliffe* fails to teach, suggest, or motivate the limitations found in claims 7 and 17.

Based on at least the foregoing reasons, therefore, Applicants respectfully submit that the cited prior art fails to anticipate or make obvious Applicants invention, as claimed for example in independent claims 2, 8, 12, and 18. Applicants note for the record that the remarks above render the remaining rejections of record for the independent and dependent claims moot, and thus addressing individual rejections or assertion with respect to the teachings of the cited art is unnecessary at the present time, but may be undertaken in the future if necessary or desirable, and Applicants reserve the right to do so. In the event that the Examiner finds any remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney.

Dated this 13th day of April, 2004.

Respectfully submitted,



RICK D. NYDEGGER
Registration No. 28,651
ERIC M. KAMERATH
Registration No. 46,081
Attorney for Applicant
Customer No. 022913

KCS0000001151V001